


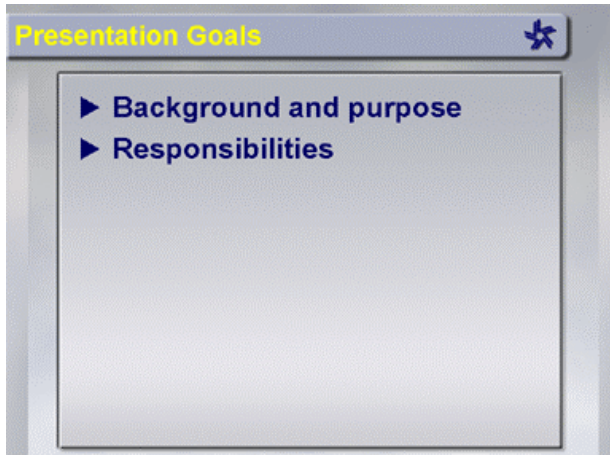
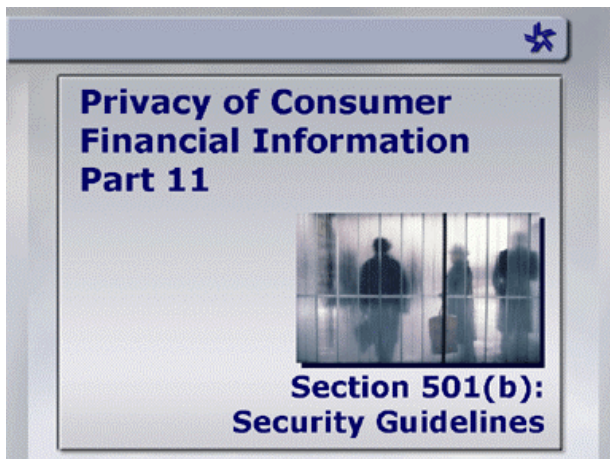
PRIVACY OF CONSUMERS' FINANCIAL INFORMATION PART 11 SECTION 501(b): SECURITY GUIDELINES

RESOURCES PROVIDED THROUGH

FFIEC InfoBase 

APRIL 2001

Slides



Narration

In this presentation, we'll look at guidelines for the institutional safeguarding of customers' non-public personal information.

First, we'll look at the background and purpose of the guidelines themselves, and then we'll discuss some specific responsibilities they address.

The security guidelines for protecting customer information were developed by an interagency group, representing all five Federal-banking, regulatory agencies,

Section 501(b)

FINANCIAL INSTITUTIONS SAFEGUARDS.— *In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—*

as mandated by Section 501(b) of the Gramm-Leach-Bliley Act.

You can use your Flash viewer to pause or rewind this presentation to facilitate reading this text.

Section 501(b)

(1) to insure the security and confidentiality of customer records and information;
(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Guideline Objective

Assure security and confidentiality of customer records and information

The objective of the guidelines is to assure security and confidentiality of customer records and of customer information.

Safeguards

Administrative



Technical



Physical



Guidelines were designed to protect against anticipated threats or hazards to the security or integrity of the records.

This includes unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to that customer.

Specifically, the guidelines establish:

- Administrative,
- Technical, and
- Physical

safeguards for the protection of customers' non-public personal information.

The key components of these guidelines are derived from existing, security-related supervisory guidance, issued previously by Federal banking regulatory agencies.

Applicability

- ▶ Customer nonpublic personal information only
- ▶ Not information relating to:
 - ▶ Bank
 - ▶ Business customers
 - ▶ Consumers



Keep in mind that security guidelines apply only to a customer's nonpublic personal information. They do not apply to information relating to the bank, business customers, or consumers who have not established an ongoing relationship with the bank.

This definition was designed to be compatible with the information covered by the privacy guidelines.

Guideline Implementation

- ▶ July 1, 2001
- ▶ Safety and soundness enforcement
- ▶ Grandfathered July 1, 2003



With a target implementation date of July first, two thousand and one, the 501(b) guidelines will be enforceable under agency safety and soundness standards, similar to the way in which Y2K guidelines were enforced.

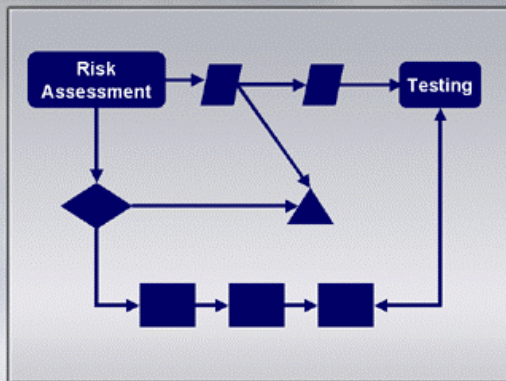
There is a two-year grandfathering stipulation, which provides that agreements with service providers will not be subject to the guidelines until July first, two thousand and three. This stipulation is applied if the bank entered into contract on or before thirty days after the publication of the guidelines, which was February first two-thousand and one.

Presentation Goals

- ▶ Background and purpose
- ▶ Requirements

Now, let's look at some of the requirements outlined in the guidelines.

Information Security as a Process



First, keep in mind that these guidelines are based on a process-oriented approach to regulation. That is, examiners should look not only at what procedures a bank is using to protect customer information, but also, and more importantly, at the process the bank used to develop those procedures.

Comprehensive Program



Risk Management

Bank management needs to implement a comprehensive, written program that is appropriate to the size and to the complexity of their bank.

The bigger the bank and the more complex its business areas, the more complex the process of implementing security procedures should be.

Requirements



The security process and resulting actions must protect against:

- ▶ Unauthorized access
- ▶ Unauthorized use
- ▶ Internal and external threats

As mentioned earlier, the bank needs to protect against both unauthorized access to customer records and information and against unauthorized use of that information.

Furthermore, the guidelines require a bank to establish this protection for potential threats from both internal and external sources.

Internal and External Threats



Internal Threats



External Threats

Internal threats would include issues such as misuse of information by employees, and external threats would include issues such as computer hacking or intrusion of the bank's computer networks.

Separate Responsibilities



Board of Directors



Management

Specific responsibilities are outlined in information security guidelines for an institution's planning process. These include separate responsibilities for the bank's board of directors and for its management team.

Board Responsibilities

- ▶ Approve program
- ▶ Oversee efforts
- ▶ Assign specific responsibilities
- ▶ Review reports
- ▶ Assess risks

According to the guidelines, the board has specific responsibilities in the information security process.

The board, or an appropriate committee of the board members, needs to approve a written information security program; and oversee efforts to develop, implement, and maintain an effective information security program.

As part of the program, the board also needs to assign specific responsibilities for implementation and to review reports from management.

And, as part of the process, the board needs to assess risks; that is, they need to identify reasonably foreseeable internal and external threats to customer information or to information systems.

Management Responsibilities



- Assessing internal and external threats
- Determining criticality of information

Management should be the likelihood and potential danger of internal and external threats as they relate to the sensitivity of the customer information being protected.

The common theme in all of management's responsibilities is simply that of risk assessment. In other words, how critical is the information that management is protecting?

Management Responsibilities



Obviously, the more critical the information, the more steps management must have in place to protect the information.

Management Responsibilities



Evaluation of:

- ▶ Policies
- ▶ Procedures
- ▶ Customer information systems
- ▶ Other risk control practices

These steps should include the evaluation of policies, procedures, customer information systems, and other arrangements that are in place to control risk.

The next presentation, *501(b) and Bank Management*, takes a more detailed look at the management responsibilities as outlined in the guidelines.